(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 745 965**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 03185**

(51) Int Cl[6] : **H 04 L 9/32**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 08.03.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 12.09.97 Bulletin 97/37.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *INSIDE TECHNOLOGIES SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** KOWALSKI JACEK.

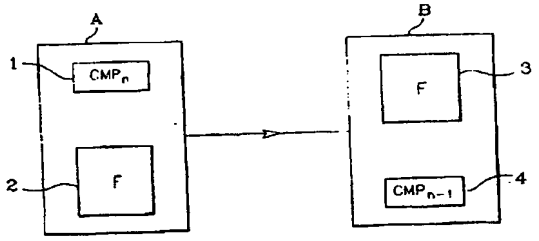
(73) **Titulaire(s) :** .

(74) **Mandataire :** CABINET BALLOT SCHMIT.

(54) PROCEDE D'AUTHENTIFICATION D'UN EMETTEUR AU COURS D'UNE COMMUNICATION A UN SEUL SENS.

(57) Procédé d'authentification d'un émetteur (A, 10, 30) par un récepteur (B, 20, 50), caractérisé en ce que, à chaque nouvelle communication, l'émetteur (A, 10, 30) envoie au récepteur la valeur (CMP_n) d'un compteur (1, 11) et un code d'authentification (CA) élaboré au moins à partir de la valeur (CMP_n) du compteur (1, 11), modifie la valeur (CMP_n, CMP_n) du compteur (1, 11) selon un sens de modification prédéterminé, le récepteur (B, 20, 50) vérifie la validité du code d'authentification (CA) envoyé par l'émetteur et vérifie que la valeur (CMP_n) du compteur reçue est différente, selon ledit sens de modification, d'une valeur (CMP_{n-1}) du compteur reçue au cours d'une communication précédente.

Application aux communications à un seul sens. Application notamment aux télécommandes et aux audiocartes.



FR 2 745 965 - A1

PROCEDE D'AUTHENTIFICATION D'UN EMETTEUR AU COURS D'UNE COMMUNICATION A UN SEUL SENS

La présente invention concerne un procédé permettant à un circuit B recevant un ordre ORD d'un circuit A, de vérifier, avant d'exécuter cet ordre ORD, que le circuit A est habilité à envoyer cet ordre.

Plus particulièrement, la présente invention concerne un tel procédé applicable au cas où le circuit A et le circuit B ne peuvent communiquer que dans le sens de A vers B.

On connaît de nombreuses applications où une communication entre deux circuits n'est possible que dans un seul sens. C'est le cas notamment des télécommandes utilisant un faisceau de lumière infrarouge ou une onde radioélectrique, et de certains types de carte à puce comme les audiocartes, prévues pour composer sur une ligne téléphonique un numéro d'accès à un service réservé.

Très souvent, un degré de sécurité est souhaitable afin d'éviter qu'un fraudeur puisse découvrir le codage particulier de l'ordre ORD envoyé par l'émetteur A. Par exemple, dans le cas d'une audiocarte, une personne pourrait mettre sur écoute la ligne téléphonique et découvrir le numéro à composer pour accéder au service réservé. Dans le cas d'une télécommande, par exemple une télécommande contrôlant l'ouverture des portes d'un véhicule, une personne pourrait enregistrer au moyen d'un capteur le code binaire envoyé par la télécommande, en vue de le reproduire.

Pour éviter ce genre de fraude, on recherche donc un moyen permettant à un récepteur B de vérifier l'authenticité d'un émetteur A avant d'exécuter l'ordre ORD

reçu, même si cet ordre ORD est en lui-même correct en ce qui concerne son codage.

On connaît déjà des procédés dits à code roulant ou "rolling code", applicables aux communications à un seul sens. Selon ces procédés, l'émetteur A s'authentifie auprès du récepteur B à chaque nouvelle communication en lui envoyant un code X_n de la forme

$$X_n = G(X_{n-1}),$$

calculé au moyen d'une fonction mathématique G et à partir du code X_{n-1} utilisé à la communication précédente. Le récepteur B, qui a conservé en mémoire le code précédent X_{n-1}, vérifie la validité du code X_n au moyen de la fonction G avant d'autoriser la nouvelle transaction ou d'exécuter un ordre reçu.

Un inconvénient de ces procédés est de nécessiter une parfaite synchronisation entre l'émetteur A et le récepteur B. En effet, si à un instant donné le code X_n envoyé par l'émetteur A n'est pas reçu par le récepteur B, A et B ne sont plus synchronisés, l'émetteur A envoyant le code X_{n+1} alors que B attend le code X_n. Les procédés à code roulant sont donc inapplicables aux systèmes à télécommande, où le signal envoyé par l'émetteur n'est pas toujours reçu du premier coup par le récepteur.

De plus, la fonction mathématique G doit être d'une grande complexité pour résister aux éventuels fraudeurs et son calcul nécessite l'intervention d'un microprocesseur. Or, pour les applications à faible coût et grand volume de production comme les télécommandes, les audiocartes, ainsi que d'autres, on souhaite utiliser des puces à logique câblée, d'un coût de revient très inférieur à celui des puces à microprocesseur.

Ainsi, un objectif de la présente invention est de prévoir un procédé d'authentification applicable à une communication à un seul sens et ne nécessitant pas de synchronisation entre l'émetteur et le récepteur.

Un autre objectif de la présente invention est de prévoir un procédé d'authentification qui puisse s'appliquer aussi bien aux puces à microprocesseur qu'aux puces à logique câblée.

Ces objectifs sont atteints grâce à un procédé d'authentification d'un émetteur par un récepteur, dans lequel, à chaque nouvelle communication, l'émetteur envoie au récepteur une valeur d'un compteur et un code d'authentification élaboré au moins à partir de la valeur du compteur, modifie la valeur du compteur selon un sens de modification prédéterminé, le récepteur vérifie la validité du code d'authentification envoyé par l'émetteur et vérifie que la valeur du compteur reçue est différente, selon le sens de modification, d'une valeur du compteur reçue au cours d'une communication précédente.

La valeur du compteur peut être toujours augmentée à chaque communication, ou toujours diminuée. Dans le premier cas, le récepteur vérifie que la valeur du compteur reçue est strictement supérieure à la valeur reçue au cours de la communication précédente. Dans le deuxième cas, que la valeur reçue est strictement inférieure à la valeur reçue au cours de la communication précédente.

De préférence, la valeur du compteur est modifiée par l'émetteur avant d'être envoyée au récepteur.

Avantageusement, le code d'authentification est élaboré par des moyens d'authentification à clef secrète. Ces moyens utilisés dans l'art antérieur pour l'authentification des cartes à puce peuvent être réalisés aussi bien sous forme de logiciel que par de la logique câblée, de sorte que le procédé de l'invention peut être mis en oeuvre avec tout type de microcircuit, à microprocesseur ou à logique câblée.

Avantageusement, le compteur est organisé en lignes de poids croissants comprenant des bits de même poids, la modification de la valeur du compteur comprenant l'étape consistant à lire le compteur bit à bit à partir des lignes de plus faible poids et changer la valeur du premier bit

rencontré dont la valeur est égale à une valeur initiale de programmation.

Ces caractéristiques, avantages ainsi que d'autres de la présente invention seront décrits plus en détail dans la description suivante du procédé de l'invention et de deux exemples d'application du procédé de l'invention, en relation avec les figures jointes parmi lesquelles :

- la figure 1 représente très schématiquement sous forme de blocs les fonctions nécessaires à la mise en oeuvre du procédé de l'invention,
- la figure 2 représente un premier exemple d'application du procédé de l'invention à un système de télécommande comprenant un émetteur à logique câblée et un récepteur à microprocesseur,
- la figure 3 représente le contenu d'une mémoire présente dans l'émetteur de la figure 2,
- les figures 4A à 4E représentent, à diverses étapes du procédé de l'invention, le contenu d'un compteur présent dans l'émetteur de la figure 2, et
- la figure 5 représente un deuxième exemple d'application du procédé de l'invention à une audiocarte.

La figure 1 représente très schématiquement les éléments fonctionnels à prévoir dans un circuit A et un circuit B pour mettre en oeuvre le procédé de l'invention. On rappelle que le procédé de l'invention a pour but de permettre la vérification par le circuit B de l'authenticité du circuit A, et que cette vérification doit être possible dans le cas où la communication de données entre A et B ne peut se faire que dans le sens de A vers B, A étant émetteur et B récepteur.

Selon l'invention, le circuit A est équipé d'un compteur 1 et d'une fonction d'authentification F représentée par un bloc 2, ces éléments pouvant être matériels ou entièrement logiciels. Le circuit B est également équipé de la fonction d'authentification F, représentée par un bloc 3, et d'une mémoire 4. La fonction F est une fonction cryptographique de tout type connu,

permettant de produire un code d'authentification CA à partir d'un code d'entrée CE, CA pouvant s'écrire :

$$CA = F(CE)$$

Le procédé selon l'invention intervient à chaque nouvelle communication entre A et B, et comprend les étapes suivantes :

(1) le circuit A modifie la valeur de son compteur 1, que l'on désignera CMP_{n-1}. La modification est faite selon un sens de modification invariable déterminé par convention et choisi une fois pour toutes. Le circuit A peut par exemple toujours incrémenter le compteur 1 d'une unité à chaque communication, ou toujours le décrémenter. La nouvelle valeur du compteur 1 est désignée CMP_n.

(2) le circuit A envoie au circuit B le contenu du compteur 1, c'est-à-dire la valeur CMP_n,

(3) le circuit A élabore, au moyen de la fonction F et d'un code d'entrée CE comprenant au moins la valeur CMP_n du compteur 1, un code d'authentification CA de la forme

$$CA = F(CMP_n)$$

et envoie ce code CA au circuit B,

(4) le circuit B élabore, au moyen de la fonction F et à partir de la valeur reçue CMP_n, un code d'authentification CA' de la forme

$$CA' = F(CMP_n)$$

(5) le circuit B compare CA à CA',

(6) le circuit B compare la valeur du compteur reçue CMP_n à la valeur CMP_{n-1} reçue au cours de la communication précédente, enregistrée dans sa mémoire 4,

(7) enfin, le circuit B enregistre la nouvelle valeur CMP_n du compteur 1 dans sa mémoire 4, par exemple à la place de CMP_{n-1}.

Selon l'invention, le circuit A est considéré comme authentique par le circuit B au terme des étapes (5) et (6) si :

- les codes d'authentifications CA et CA' sont identiques, et si
- la valeur CMP_n du compteur 1 reçue est différente, selon le sens de modification imposé, de la valeur CMP_{n-1} reçue lors de la communication précédente. En d'autres termes, le circuit B vérifie que la valeur CMP_n est strictement supérieure à CMP_{n-1} dans le cas où l'on choisit d'incrémenter le compteur 1 à chaque nouvelle communication, ou strictement inférieure à CMP_{n-1} si l'on choisit de décrémenter le compteur 1 à chaque nouvelle communication.

Ainsi, la sécurité offerte par le procédé de l'invention repose sur un double mécanisme. D'une part, la vérification de la validité du code d'authentification CA permet de s'assurer que l'émetteur A possède bien la fonction d'authentification F. D'autre part, le fait d'imposer une valeur CMP_n sans cesse croissante ou sans cesse décroissante comme code d'entrée CE de la fonction d'authentification F permet de garantir un renouvellement permanent du code d'authentification CA et d'écarter tout risque de fraude par imitation du code CA.

Le procédé de l'invention présente en outre l'avantage de ne pas nécessiter de synchronisation entre A et B. En effet, si après une ou plusieurs communications manquées entre A et B le circuit B possède dans sa mémoire 3 une valeur de comptage CMP_{n-1} ayant un retard de plusieurs incréments (ou plusieurs décréments) par rapport à la valeur CMP_n présente dans le compteur 1 du circuit A, le circuit B peut quand même reconnaître l'authenticité du circuit A puisqu'il vérifie simplement que la valeur reçue CMP_n est strictement supérieure à CMP_{n-1} (ou strictement inférieure, selon le sens de modification choisi).

Toutefois, si cela pouvait présenter un intérêt dans certaines applications, on pourrait imposer une

synchronisation entre A et B en exigeant que l'écart entre deux valeurs de compteur CMP_{n-1}, CMP_n reçues successivement par le circuit B soit strictement égal à un seul incrément (ou un seul décrément).

D'autre part, l'étape (1) de modification du compteur 1 pourrait être réalisée après l'étape (3) d'envoi du contenu du compteur, à la condition de prévoir au moment de la mise en service du système un décalage d'au moins un incrément entre la valeur initiale présente dans la mémoire 4 et la valeur initiale du compteur 1, afin que A puisse être reconnu par B à la première communication.

Les caractéristiques générales du procédé selon l'invention étant décrites, on va maintenant s'intéresser à sa mise en oeuvre pratique. Comme on l'a indiqué au préambule, on souhaite notamment appliquer le procédé de l'invention aux microcircuits à logique câblée.

Ainsi, et c'est un aspect de la présente invention, on propose de produire le code d'authentification CA au moyen d'un circuit d'authentification à clef secrète Ks du type utilisé dans l'art antérieur pour l'authentification des cartes à mémoire. Dans leur application classique, les circuits d'authentification à clef secrète sont intégrés dans les puces des cartes à mémoire et ont pour fonction de transformer un mot aléatoire ou aléa ALEXT envoyé par un terminal en un code d'authentification CA. Le fonctionnement des circuits d'authentification à clef secrète Ks repose généralement sur des opérations successives de lecture d'une mémoire non accessible depuis l'extérieur, dans laquelle est stockée une pluralité de mots binaires représentant la clef secrète Ks. Ce fonctionnement peut par ailleurs être simulé par logiciel, de sorte que l'on a le choix entre une implantation matérielle (logique câblée) ou une implantation logicielle (microprocesseur) des fonctions d'authentification F_{Ks} à clef secrète Ks. Des exemples de réalisation sont donnés dans les brevets français FR 92 13913 et FR 89 09734, ainsi que dans la demande de brevet français FR 95 12176 au nom

de la demanderesse dans laquelle il est proposé un circuit d'authentification très résistant à la fraude.

La figure 2 représente une application du procédé de l'invention à un système de télécommande comprenant un microcircuit émetteur 10 à logique câblée et un circuit récepteur 20 à microprocesseur.

Le microcircuit 10 comprend un compteur 11, un circuit d'authentification 12 à clef secrète Ks, une diode électroluminescente infrarouge 13 et un circuit de commande 14 de la diode 13. Un séquenceur câblé 15 contrôle le fonctionnement de l'ensemble. Un interrupteur 16 externe actionnable par un utilisateur permet de mettre le microcircuit 10 sous tension, l'interrupteur 16 étant par exemple raccordé à une pile électrique 17. Le circuit d'authentification 12 est piloté par un signal d'horloge H délivré par le séquenceur 15, et présente une entrée série 12-1 destinée à recevoir un code d'entrée CE et une sortie série 12-2 pour délivrer un code d'authentification CA de la forme $F_{Ks}(CE)$. De façon classique, la clef secrète Ks est stockée dans une zone mémoire 12-3 non accessible de l'extérieur.

Le compteur 11 est ici une zone 11 d'une mémoire 18 de type EEPROM effaçable et programmable électriquement. Cette zone mémoire 11 présente une structure en lignes et en colonnes que l'on aperçoit sur les figures 4A à 4E décrites plus loin, et est accessible bit par bit en lecture et en écriture par l'intermédiaire d'un décodeur 18-1 de lignes et d'un décodeur 18-2 de colonnes commandés par le séquenceur 15.

Le récepteur 20 comprend un microprocesseur 21, une mémoire programme 22 de type ROM, une mémoire de données 23 non volatile de type RAM sauvegardée ou de type EEPROM, un détecteur infrarouge 24 et un circuit 25 de mise en forme des signaux reçus par le détecteur 24. La mémoire programme 22 contient des instructions PGR de fonctionnement du microprocesseur 21 et un programme PF_{Ks} de simulation du

circuit d'authentification 12 de l'émetteur 10, permettant de calculer la fonction d'authentification F_{Ks}.

Lorsque l'interrupteur 16 est fermé, le séquenceur 15 exécute les tâches pour lesquelles il a été câblé. Le séquenceur 15 commence tout d'abord par modifier la valeur CMP_{n-1} du compteur 11, d'une manière qui sera décrite en détail plus loin. La nouvelle valeur du compteur est CMP_n. Ensuite, le séquenceur 15 aiguille la sortie de la mémoire 18 sur le circuit 14 de commande de la diode 13 ainsi que sur l'entrée 12-1 du circuit d'authentification 12, et déclenche la lecture bit à bit du compteur 11 (c'est-à-dire de la zone de la mémoire 18 utilisée comme compteur 11), tout en envoyant des signaux d'horloge H au circuit d'authentification 12. Le contenu CMP_n du compteur 11 est donc envoyé au récepteur 20 sous forme de lumière infrarouge et simultanément absorbé par le circuit d'authentification 12 en tant que code d'entrée CE. Lorsque cette opération est terminée, le séquenceur 15 continue d'activer le circuit d'authentification 12 et aiguille sa sortie 12-2 sur le circuit 14. Le circuit d'authentification 12 délivre un code d'authentification CA de la forme

$$CA = F_{Ks}(CMP_n)$$

qui est envoyé au récepteur 20 sous forme de lumière infrarouge.

Dans le récepteur 20, le microprocesseur 21 lit la valeur CMP_n et le code CA à la sortie du circuit 25 et les stocke dans la mémoire 23 qui contient déjà la valeur CMP_{n-1} reçue à la communication précédente. Conformément à l'invention, le microprocesseur 21 calcule un code CA' à partir de CMP_n, vérifie que le code CA reçu est identique à CA' calculé, et que la valeur CMP_n est supérieure, ou inférieure, selon la convention choisie, à CMP_{n-1}. Si les deux conditions sont réunies, le microprocesseur 20 envoie un signal de validation VAL qui peut être utilisé à

diverses fins, par exemple pour l'ouverture des portes d'une automobile, la mise hors tension ou sous tension d'un système d'alarme, etc.

Dans un système de télécommande du type "ouverture de porte", il n'est pas nécessaire d'envoyer au récepteur 20 d'autres informations que les données d'authentification $\{CMP_n, F_{Ks}(CMP_n)\}$. En effet, ces données représentent à elles seules un ordre ORD dans la mesure où elles conduisent à une reconnaissance de l'authenticité de l'émetteur 10. Toutefois, dans un système de télécommande à ordres multiples (par exemple une télécommande d'un système complexe comme une télévision) il peut être nécessaire d'envoyer au récepteur un (ou plusieurs) code ORD_y choisi parmi une pluralité de codes ORD1, ORD2, ORD3... possibles, représentant l'ordre particulier à exécuter. Le code ORD_y peut être envoyé séparément après les données d'authentification, mais il est avantageux d'utiliser ORD_y comme donnée d'authentification, de manière à augmenter la complexité du code d'authentification CA et rendre le système de télécommande encore plus résistant à la fraude. En pratique, cela consiste à chaîner le code ORD_y à la valeur CMP_n en entrée du circuit 12 et produire un code d'authentification CA du type

$$CA = F_{Ks}\ (CMP_n,\ ORD_y)$$

Les données envoyées étant alors :

$$\{CMP_n,\ ORD_y,\ CA\}$$

Le microprocesseur 20 utilise tout d'abord le code ORD_y comme une donnée d'authentification lui permettant de vérifier le code CA reçu, puis lorsque l'authentification est terminée, "interprète" le code ORD_y pour réaliser l'opération demandée par l'émetteur 10.

D'autre part, il est envisageable que le récepteur 20 doive répondre à différents émetteurs 10 ayant chacun leur

clef secrète Ks. C'est le cas notamment lorsque le récepteur 20 est mis à la disposition de plusieurs usagers dans un lieu public. Dans ce cas, le récepteur 20 ne connaît pas la clef secrète Ks de l'émetteur 10 et la détermine à partir d'un numéro d'identification NI de l'émetteur selon la relation suivante :

$$Ks = F_{Kp} (NI)$$

F_{Kp} étant une fonction de transformation à clef secrète Kp implantée dans le récepteur 20. Dans ce cas, le numéro d'identification NI de l'émetteur 10 est stocké dans la mémoire 18, comme représenté en figure 3, et est incorporé dans le message envoyé par l'émetteur 10 qui est de la forme :

$$\{NI, CMP_n, CA\}$$

Le code d'authentification CA peut être élaboré à partir de la valeur CMP_n du compteur 11, comme décrit précédemment, ou à partir d'un code d'entrée CE formé par chaînage de NI et CMP_n, ce qui permet d'augmenter le brouillage. Le code CA est alors de la forme :

$$CA = F_{Ks} (NI, CMP_n)$$

De plus, si un ordre particulier ORD_y doit être émis, cet ordre ORD_y peut être chaîné, comme proposé précédemment, aux autres données formant le code d'entrée CE, le code d'authentification CA étant alors de la forme :

$$CA = F_{Ks} (NI, CMP_n, ORD_y)$$

et le message envoyé de la forme :

$$\{NI, CMP_n, ORD_y, CA\}$$

On va maintenant décrire, à titre d'exemple, un mode de réalisation du compteur 11. Le procédé de l'invention nécessitant une évolution de la valeur du compteur 11 à chaque communication, toujours dans le même sens, il faut que la capacité du compteur 11 soit suffisante pour assurer le comptage des communications pendant toute la durée de vie de l'émetteur 10. Par exemple, un compteur 11 pouvant compter de 0 à 36000 permettrait d'utiliser l'émetteur 10 fois par jour pendant 10 ans. Toutefois, le compteur 11 doit être d'un faible encombrement.

Les figures 4A à 4E donnent un exemple de gestion de la zone 11 de la mémoire 18 offrant une grande capacité de comptage à partir d'un nombre limité de bits. Le compteur 11 comprend 6 lignes L1, L2, L3, L4, L5, L6 de poids croissant comprenant chacune 8 bits B0, B1,...B7 de même poids. Au départ, tous les bits B0-B7 de chaque ligne L1-L6 sont programmés à une valeur initiale, par exemple à "1" comme montré en figure 4A. La modification de la valeur du compteur 11 à chaque nouvelle communication est réalisée de la façon suivante. Le séquenceur 15 lit le compteur 11 bit par bit, en commençant par les lignes de plus faible poids L1, L2,... jusqu'à trouver un bit égal à la valeur initiale de programmation, c'est-à-dire ici un bit à "1". Lorsque ce bit est trouvé, le séquenceur 15 met ce bit à "0" et remet à "1" tous les bits de toutes les lignes de plus faible poids. Par exemple, sur la figure 4B, le premier bit à "1" rencontré est le bit B0/L2. Le séquenceur 15 met à "0" ce bit et met à "1" tous les bits de la ligne L1, comme montré en figure 4C. Sur la figure 4D, le premier bit à "1" rencontré est le bit B3/L3. Le séquenceur met à "0" ce bit et met à "1" tous les bits des lignes L1 et L2 comme montré en figure 4E.

Ce mode de gestion du compteur 11 correspond à un comptage en base N+1, N étant le nombre de bits par ligne, soit ici un comptage en base 9 puisque chaque ligne comprend 8 bits. Ainsi, dans l'exemple représenté, 531440

modifications du compteur 11 sont possibles jusqu'à ce que tous les bits soient à "0".

D'autres modes de gestion du compteur 11 peuvent être envisagés. Par exemple, le comptage peut être fait en base 8. Ce comptage consiste à mettre à "0" le premier bit à "1" rencontré, comme décrit précédemment, et à mettre à "1" tous les bits sauf le premier B0 de toutes les lignes de plus faible poids. Dans ce cas, on peut compter jusqu'à 299592. Encore un autre mode de gestion consiste à mettre à "1" uniquement les bits de la ligne de poids immédiatement inférieur. Dans ce dernier cas, on n'exploite pas tous les états logiques possibles du compteur mais l'opération de modification de la valeur du compteur est simplifiée.

On notera que l'opération de modification de la valeur compteur 11 qui vient d'être décrite selon plusieurs variantes peut être assimilée à une incrémentation ou une décrémentation selon la convention choisie. Si par convention les bits à "0" sont pris en compte pour déterminer la valeur du compteur 11, la configuration initiale du compteur 11 représentée en figure 4A correspond à une valeur nulle et l'opération est une incrémentation. Si à l'inverse les bits à "1" sont pris en compte pour déterminer la valeur du compteur 11, la configuration initiale de la figure 4A correspond à la valeur maximale du compteur 11 et l'opération décrite est une décrémentation.

Dans ce qui précède, on a décrit un exemple d'application du procédé de l'invention à un système de télécommande. Il apparaîtra clairement à l'homme de l'art que la présente invention peut faire l'objet de nombreuses autres applications et modes de réalisation.

A titre d'exemple, la figure 5 illustre une application du procédé de l'invention à une audiocarte de type synchrone et représente le microcircuit 30 d'une telle audiocarte.

Le microcircuit 30 comprend, comme l'émetteur de la figure 2, une mémoire 31 de type EEPROM, un circuit d'authentification 32 à clef secrète Ks réalisant la

fonction F_{Ks}, et un séquenceur câblé 33. Le microcircuit 30 comporte ici des plots de connexion électrique parmi lesquels on distingue un plot H de réception d'un signal d'horloge, un plot RST de remise à zéro du microcircuit, un plot OUT pour l'envoi de données, et deux plots d'alimentation électrique Vcc et GND.

Selon l'invention, la mémoire 31 comprend des données TY, DA, NI et CPM_n. Les données TY identifient le type de la carte, les données DA représentent le numéro d'appel d'un service téléphonique SVR auquel la carte permet d'accéder, les données NI représente le numéro d'identification (ou numéro de série) du microcircuit 30, et enfin CMP_n représente la valeur du compteur 11 déjà décrit.

Lorsque l'audiocarte est insérée dans un terminal 40, le terminal 40 applique le signal d'horloge H au séquenceur 33 et lit sur le plot OUT les données TY. Ces données lui permettent de savoir qu'il est en présence d'une audiocarte, et vont déterminer son fonctionnement au cours des séquences suivantes (on suppose ici que le terminal est polyvalent et peut accepter divers types de cartes). Ensuite, le terminal 40 applique à nouveau le signal d'horloge H pour lire dans la mémoire 31 les données DA, à partir desquelles il compose sur une ligne téléphonique 41 le numéro du service distant SVR à appeler.

Lorsque le service SVR est atteint, le terminal 40 ferme un interrupteur 42 de manière à connecter la sortie OUT du microcircuit 30 à la ligne téléphonique 41 et applique le signal d'horloge au séquenceur 33 jusqu'à ce que le compteur 11 soit incrémenté et les données d'authentification suivantes envoyées sur la ligne 41 :

$$\{NI, CMP_n, CA\}$$

Le code d'authentification CA peut être élaboré à partir de CMP_n ou, mieux encore, de NI et CMP_n de manière à augmenter le brouillage:

$$CA = F_{Ks} (NI, CMP_n)$$

Une variante permettant d'augmenter plus encore la complexité du code d'authentification CA consiste à injecter dans le circuit 32 toutes les données pouvant se trouver dans la mémoire 31, CA étant alors de la forme :

$$CA = F_{Ks} (TY, DA, NI, CMP_n)$$

Dans cas il convient d'incorporer TY et DA aux données d'authentification envoyées sur la ligne 41 :

$$\{TY, DA, NI, CMP_n, CA\}$$

A l'autre extrémité de la ligne 41, les données d'authentification sont reçues par un circuit de contrôle 50 qui bloque l'accès au service SVR.

Conformément au procédé de l'invention, le circuit 50 détermine tout d'abord la clef secrète Ks du microcircuit 30 au moyen du numéro d'identification NI reçu et de sa propre clef secrète Kp, de la manière déjà décrite. Puis, le circuit 50 vérifie la validité du code d'authentification CA reçu, et enfin s'assure que la valeur CMP_n du compteur 11 émise par le microcircuit 30 est strictement différente, selon le sens de modification du compteur 11 choisi par convention, de la valeur CMPn-1 reçue à la communication précédente. Si ces conditions sont remplies, le circuit 50 ferme un interrupteur 51 qui libère l'accès au service SVR.

REVENDICATIONS

1. Procédé d'authentification d'un émetteur (A,10,30) par un récepteur (B,20,50), caractérisé en ce que, à chaque nouvelle communication,

l'émetteur (A,10,30) :

- envoie au récepteur la valeur (CMP_n) d'un compteur (1,11) et un code d'authentification (CA) élaboré au moins à partir de la valeur (CMP_n) dudit compteur (1,11),
- modifie la valeur (CMP_{n-1}, CMP_n) du compteur (1,11) selon un sens de modification prédéterminé,

le récepteur (B,20,50) :

- vérifie la validité du code d'authentification (CA) envoyé par l'émetteur et
- vérifie que la valeur (CMP_n) du compteur reçue est différente, selon ledit sens de modification, d'une valeur (CMP_{n-1}) du compteur reçue au cours d'une communication précédente.

2. Procédé selon la revendication 1, caractérisé en ce que la valeur du compteur (1,11) est toujours augmentée à chaque communication, le récepteur (B,20,50) vérifiant que la valeur (CMP_n) du compteur reçue est strictement supérieure à la valeur (CMP_{n-1}) reçue au cours de la communication précédente.

3. Procédé selon la revendication 1, caractérisé en ce que la valeur du compteur (1,11) est toujours diminuée à chaque communication, le récepteur (B,20,50) vérifiant que la valeur (CMP_n) du compteur reçue est strictement inférieure à la valeur (CMP_{n-1}) reçue au cours de la communication précédente.

4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que la valeur (CMP_{n-1}) du compteur (1,11) est modifiée par l'émetteur (A,10,30) avant d'être envoyée au récepteur (B,20,50).

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que ledit code d'authentification (CA) est élaboré par des moyens (12, 32) d'authentification (F_{Ks}) à clef secrète (Ks).

6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce que ledit compteur (11) est organisé en lignes (L1-L6) de poids croissants comprenant des bits (B0-B7) de même poids, la modification de la valeur du compteur (11) comprenant l'étape consistant à lire le compteur (11) bit à bit à partir des lignes (L1) de plus faible poids et changer la valeur du premier bit rencontré (B0/L2, B3/L3) dont la valeur est égale à une valeur initiale de programmation ("1").

7. Procédé selon la revendication 6, caractérisé en ce que la modification de la valeur du compteur (11) comprend en outre l'étape consistant à programmer à ladite valeur initiale de programmation ("1") les bits d'au moins une ligne de poids plus faible que la ligne comprenant ledit premier bit.

8. Procédé selon la revendication 6, caractérisé en ce que la modification de la valeur du compteur (11) comprend en outre l'étape consistant à programmer à la valeur ("1") initiale de programmation les bits (B1-B7) sauf le premier (B0) de toutes les lignes de poids plus faible que la ligne comprenant ledit premier bit.

9. Système de télécommande comprenant un émetteur (10) et un récepteur (20) mettant en oeuvre le procédé selon l'une des revendications 1 à 8.

10. Système de communication téléphonique comprenant une audiocarte (30) et un circuit (50) de contrôle de l'accès à un service réservé mettant en oeuvre le procédé selon l'une des revendications 1 à 8.

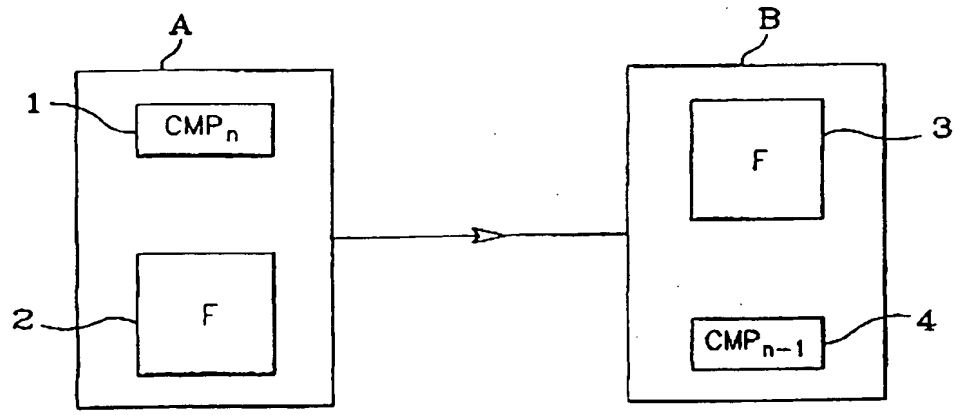


FIG.1

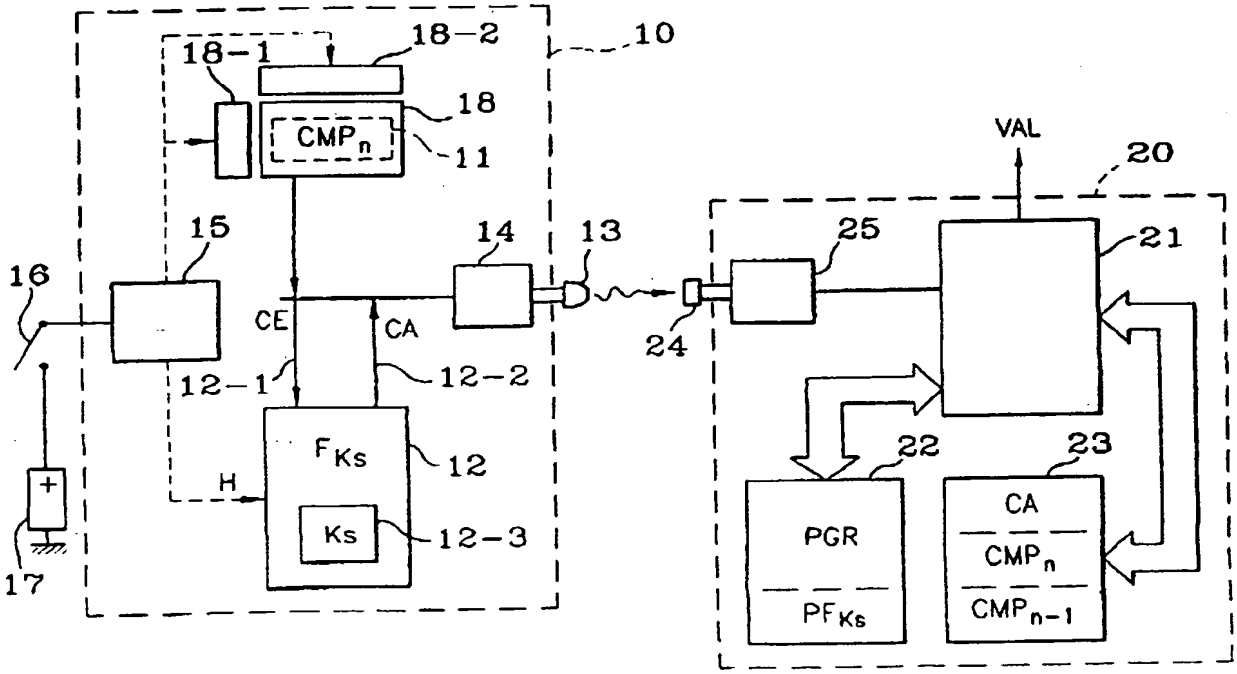


FIG.2

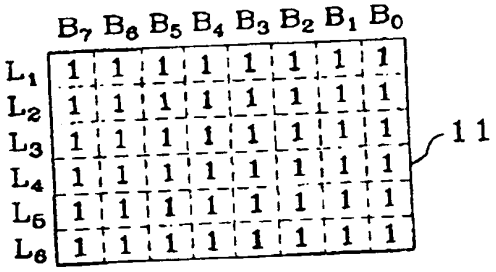


FIG.4A

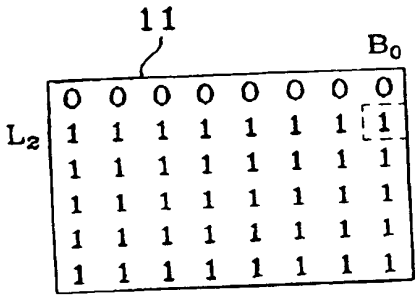


FIG.4B

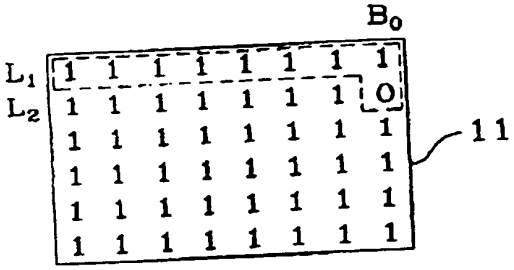


FIG.4C

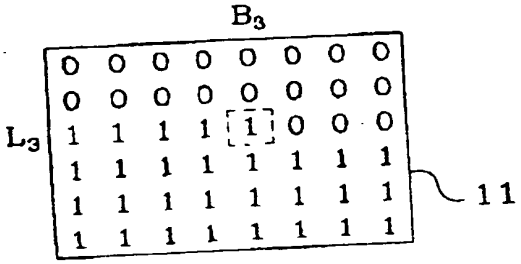


FIG.4D

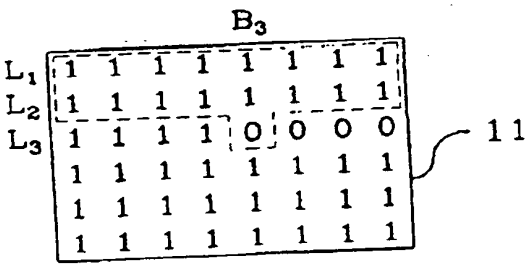


FIG.4E

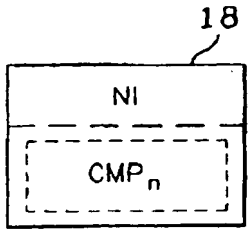


FIG.3

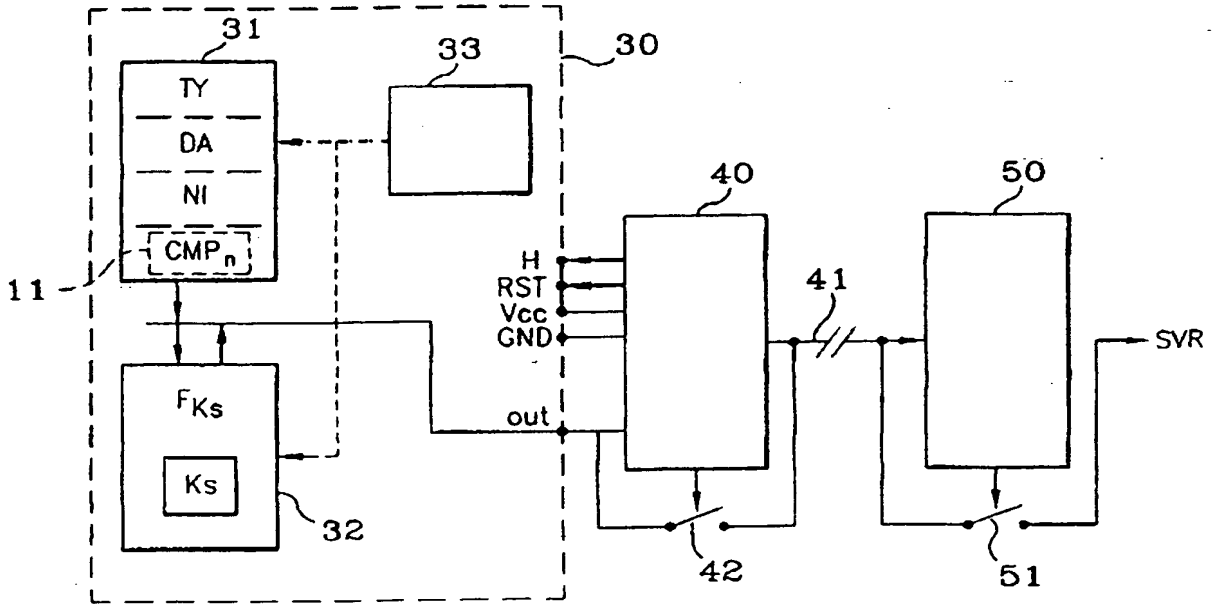


FIG.5

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2745965
N° d'enregistrement national

FA 526427
FR 9603185

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	WO-A-95 08039 (ROCKWELL INTERNATIONAL) * abrégé * * page 1, ligne 9 - ligne 18 * * page 3, ligne 8 - ligne 19 * * page 4, ligne 10 - page 5, ligne 21 * * revendications 1-3 * * figures 1,5 * ---	1,2,4,5, 9,10
X	EP-A-0 244 332 (SOUM) * page 2, ligne 11 - page 7, ligne 18 * * figure 1 * ---	1,2,4,5, 9,10
X	EP-A-0 459 781 (NANOTEQ)	1,2,4,9, 10
A		6
	* abrégé * * colonne 3, ligne 40 - colonne 4, ligne 19 * * colonne 4, ligne 49 - colonne 5, ligne 5 * * colonne 8, ligne 45 - colonne 9, ligne 1 * * colonne 9, ligne 33 - colonne 10, ligne 7 * * colonne 10, ligne 4411 - colonne 45 * * figures 1,2 * -----	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
H04L E05B

Date d'achèvement de la recherche: 4 Décembre 1996

Examinateur: Lydon, M

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)